应用离散数学

杭州电子科技大学

代数结构

定义8 (代数系统)

非空集合G和G上的k个代数运算$f_1, \cdots, f_k$(其中f_i是n_i元代数运算)组成的系统称为**代数系统**，简称**代数**，记为$\langle G, f_1, \cdots, f_k \rangle$，而$\langle n_1, \cdots, n_k \rangle$称为该代数系统的**类型**。

定义11（半群）

设G是非空集合，$*$是G上的二元运算。如果$*$满足结合律，则称$\langle G,*\rangle$是半群。

若半群$\langle G,*\rangle$中存在单位元，则称$\langle G,*\rangle$是有幺半群。

	$\langle\mathbb{N},+\rangle$	$\langle\mathbb{N},\times\rangle$	$\langle\mathbb{R},-\rangle$	$\langle\mathbb{R}^*,\div\rangle$
半群	是	是	否	否
有幺半群	是	是		
	$\langle\mathbb{Z}_m,\times_m\rangle$	$\langle M_n(R),+\rangle$	$\langle\hat{M}_n(R),\times\rangle$	$\langle\rho(X),\cup\rangle$
半群	是	是	是	是
有幺半群	是	是	是	是

习题1

设集合

$$G=\left\{\left.\begin{pmatrix} a_{11} & a_{12} \\ 0 & 0 \end{pmatrix}\right| a_{11}, a_{12} \in \mathbb{R}\right\}$$

$*$表示矩阵乘法，试问$\langle G, *\rangle$是否是半群，是否是有幺半群？

定义12 (群)

设$\langle G,*\rangle$是有幺半群，如果$\forall x\in G$，都存在逆元$x^{-1}\in G$，则称$\langle G,*\rangle$是群。

1. G非空
2. $*$是G上的运算
3. $*$满足结合律
4. 存在单位元
5. G中的每个元素都有逆元

若$\langle G,*\rangle$是群且$*$满足交换律，则称$\langle G,*\rangle$为交换群或阿贝尔群

	$\langle \mathbb{N}, + \rangle$	$\langle \mathbb{R}, + \rangle$	$\langle \mathbb{N}, \times \rangle$	$\langle \mathbb{R}, \times \rangle$	$\langle \mathbb{R}^*, \times \rangle$
群	$\times$	$\checkmark$	$\times$	$\times$	$\checkmark$
	$\langle \mathbb{Z}_m, +_m \rangle$	$\langle \mathbb{Z}_m, \times_m \rangle$	$\langle M_n(R), + \rangle$	$\langle M_n(R), \times \rangle$	$\langle \hat{M}_n(R), + \rangle$
群	$\checkmark$	$\times$	$\checkmark$	$\times$	$\times$
	$\langle \hat{M}_n(R), \times \rangle$	$\langle \rho(X), \cap \rangle$	$\langle \rho(X), \cup \rangle$		
群	$\checkmark$	$\times$	$\times$		

习题3

在整数集合$\mathbb{Z}$上定义运算$*$如下

$$x * y = x + y - 2, \forall x, y \in \mathbb{Z}$$

判断$\langle \mathbb{Z}, * \rangle$是否是群？

例4.11

设$\langle G, * \rangle$是群，$\forall a \in G$，定义$G \to G$的映射f_a如下：

$$f_a(x) = x * a, \forall x \in G$$

令$H = \{f_a | a \in G\}$，证明$\langle H, \circ \rangle$ 是群，其中$\circ$表示复合运算。

定义13 (幂)

设$\langle G, *\rangle$是半群，$x \in G, n \in \mathbb{Z}^+$，定义

$$x^n = \begin{cases} x & n = 1 \\ x^{n-1} * x & n \geq 2 \end{cases}$$

若$\langle G, *\rangle$还是有幺半群，e为单位元，则定义$x^0 = e$

若x在G中存在逆元x^{-1}，则定义

$$x^{-n} = (x^{-1})^n.$$

例9

- 分别在群$\langle \mathbb{R}^*, \times \rangle, \langle \mathbb{R}, + \rangle$中计算$0.5^4, 0.5^0, (-2)^3, (-2)^{-3}$
- 分别在$\langle \hat{M}_r(R), \times \rangle, \langle M_2(R), + \rangle$中计算$\begin{pmatrix} 0.5 & 0 \\ 0 & 0.5 \end{pmatrix}$的*2*、-*1*，-*2*次幂

定理3

设$\langle G, * \rangle$是一个群，则

- $\forall x \in G, (x^{-1})^{-1} = x;$
- $\forall x, y \in G, (x * y)^{-1} = y^{-1} * x^{-1};$
- $\forall m, n \in \mathbb{Z}, x^m * x^n = x^{m+n}, (x^m)^n = x^{mn};$

定义14 (有限群、无限群、阶数、平凡群)

设$\langle G,*\rangle$是一个群，如果G是有限集合，则称$\langle G,*\rangle$是有限群，G中元素的个数被称为其阶数，记为$|G|$。阶等于1的群被称为平凡群，即其只有一个元素(单位元)。若G是无限集合，则称$\langle G,*\rangle$是无限群。

定义15 (次数)

设$\langle G, * \rangle$是一个群，e为其单位元。对于$x \in G$，使得$x^n = e$成立的最小正整数n被称为是x的次数，记为$|x| = n$。若不存在这样的正整数n，则称x是无限次元。

注1 (若$\langle G, * \rangle$是一个群，$x \in G$且$|x| = n$，则)

- $x^n = e$;
- $x^k \neq e, k = 1, 2, \cdots, n-1$;

例10 (证明$\mathbb{Z}_7^* = \{1,2,3,4,5,6\}$在$\times_7$运算下构成群,并求出各个元素的逆元以及次数)

$\times_7$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

定理4（方程的唯一可解性）

设$\langle G,*\rangle$是一个半群，则$\langle G,*\rangle$是群的充要条件是：$\forall a,b\in G$，方程$a*x=b, x*a=b$在G中都有唯一解。

定理5

设$\langle G,*\rangle$是一个群，e为单位元，则

- 若$|G|>1$，则$\langle G,*\rangle$没有零元；

定理6 (消去律)

设$\langle G,*\rangle$是群，则运算$*$在G上满足消去律。

即$\forall x,y,z\in G$，有

$$x*y=x*z\Rightarrow y=z,\qquad y*x=z*x\Rightarrow y=z$$

例4.15

设$\langle G,*\rangle$是有限群，$G=\{x_1,\cdots,x_n\}$。令

$$x_iG=\{x_i*x_j|j=1,2,\cdots,n\}$$

证明$x_iG=G$。

定理7

设$\langle G,*\rangle$是群，e为单位元，$a\in G$且$|a|=n$，则

1. $a^k=e$的充要条件是$n\mid k$;
2. $|a^k|=\frac{n}{\gcd(k,n)}=\frac{\operatorname{lcm}(k,n)}{k}$;
3. $|a|=|a^{-1}|$;
4. $a^s=a^t$的充要条件是$s\equiv t \mod n$;

例12

设$\langle G,*\rangle$是群，e是单位元，$a\in G$且$|a|=12$，

1. 求a^2,a^5,a^{-3}的次数;
2. 求整数$t, 0\le t\le 11$，使得$a^{-14}=a^t$;
3. 求所有满足$a^t=a^7$的整数t;

作业 习题4.3 第 2，6，8 题